Mobile malware hits ActiveSync-only devices

Mobile platforms have leapfrogged PC security for years, but as mobile device adoption explodes worldwide, these platforms face more security threats than ever before. While mobile devices are still safer than PCs, hackers are relentlessly searching for new ways to exploit these operating systems and gain access to their valuable data. Four major threats are currently targeting iOS and Android devices using very clever tactics. In fact, users may not know their devices have been compromised until after their data has been hacked.

MobileIron

MKT-9585 V1.2

Enterprises that only use ActiveSync to deploy email are particularly vulnerable to these threats because ActiveSync offers a limited range of MDM features. Many of these features apply only to older Windows operating systems, and some don't work on iOS or Android at all.[1] Only an enterprise mobility management (EMM) provider like MobileIron protects against mobile malware threats like Stagefright, Keyraider, XcodeGhost, and YiSpecter.

Only an EMM provider like MobileIron can protect your enterprise apps and data from mobile malware like Stagefright, Keyraider, XcodeGhost, and YiSpecter.

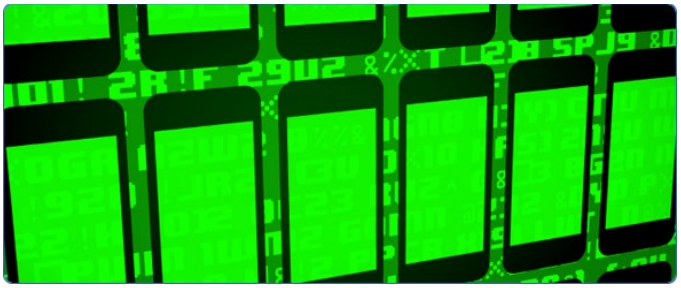
Stagefright Targets 99 Percent of Android Devices

- **How it works:** Stagefright takes advantage of a vulnerability found in the Android media library. The attacker sends a malicious multimedia message via MMS. When the vulnerable Android device receives the message, it is automatically downloaded and infects the device through the multimedia preview function. It's important to note that the user doesn't have to do anything, such as click a link or download an app, for the malicious code to wind up on their phone. It happens as soon as the MMS is received.
- **How it impacts your business:** Enterprises should be on high alert because Stagefright can steal data, hijack the microphone, use the camera, and essentially behave like spyware on the infected device.

XcodeGhost Attacks any iOS Devices with Thousands of Infected Apps

- **How it works:** XcodeGhost attacks both jailbroken and non-jailbroken devices with infected apps that have made it into the Apple App Store. Apps are accidentally infected with XcodeGhost when iOS (and OS X) developers download Apple's Xcode SDK from malicious sites other than the official Apple download site. When developers use one of these compromised versions of Xcode to develop their apps, they are unknowingly hiding malware in their apps. To date, more than 4,000 XcodeGhost apps have been identified by our partner, FireEye, and removed from the App Store by Apple.
- **How it impacts your business:** If employees download apps infected with XcodeGhost to personal or corporate-owned mobile devices, your business data could be at serious risk. The Ghost malware can allow remote command and control (CnC), open web pages on the device, fake password prompts, and steal credentials.

1 *Beehler, Eric. "Using Microsoft Exchange ActiveSync for MDM: What you can and can't do." http://searchmobilecomputing.techtarget.com/tip/Using-Microsoft-Exchange-ActiveSync-for-MDM-What-you-can-and-cant-do*



Keyraider has Stolen Data from More than 225,000 Apple Accounts

- **How it works:** KeyRaider targets jailbroken devices because jailbreaking eliminates many of the built-in security features of the operating system. It can steal usernames, passwords, certificates, and even private keys.
- **How it impacts your business:** Enterprises should be especially vigilant about blocking access to corporate information on jailbroken mobile devices. Malware like Keyraider can take control of an iPhone or iPad and quickly access corporate email, documents, and other data.

YiSpecter Secretly Harvests User Data on the Device

- **How it works:** YiSpecter infects both jailbroken and non-jailbroken devices using private APIs, which are unpublished or unsupported Apple iOS APIs. Although apps using these APIs are usually blocked during Apple’s app vetting processes, YiSpecter can be spread in three other ways: through ISPs, a worm on Windows that infects the device when pairing, and through offline app installation.
- **How it impacts your business:** Once the iOS device is infected, YiSpecter can modify, install, and launch iOS apps without the user’s permission. It can also replace existing apps with those it downloads, display full-screen ads when the user launches a normal app, change Safari’s default search engine, bookmark and open web pages, and upload device information to the CnC server. The malware can also automatically reappear after it’s been deleted.[2]

2 *Xiao, Claud. “YiSpecter: First iOS Malware that Attacks Non-jailbroken Devices by Abusing Private APIs.” Oct. 4, 2015. http://researchcenter.paloaltonetworks.com/2015/10/yispecter-first-ios-malware-attacks-non-jailbroken-ios-devices-by-abusing-private-apis/*

Secure Mobile Devices from Malware with MobileIron

Although ActiveSync is great for quickly enabling email on mobile devices, it leaves your business wide open to mobile malware attacks on iOS and Android. MobileIron provides the security you need to block these threats on all your managed devices.

MobileIron Detects and Mitigates Threats

MobileIron helps eliminate many of these threats by first determining the posture, or security status, of the device. Posture checks ensure the device isn't jailbroken, that both the device and user are authorized to access the network, and that the device contains approved apps and OS versions. Only devices with a compliant security posture are allowed to access corporate information on the device or through the network.

If MobileIron detects malware on a device, MobileIron automatically takes compliance actions to quarantine the device, remove corporate data, and prevent further access to corporate data from that device.

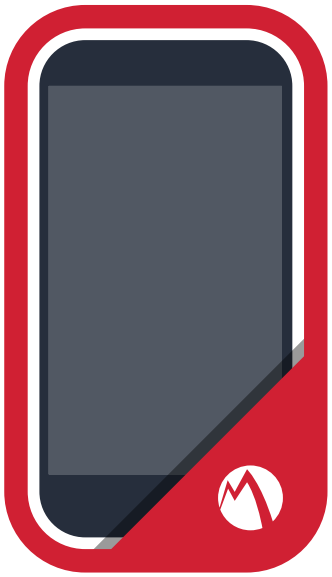
Secured with MobileIron:

- OS version identification
- Jailbreak and root detection
- App version detection
- Block unmanaged app access
- Conditional device access (block network access)
- Compliance actions / Device quarantine
- Selective wipe of business apps and data
- Detected threat notifications and alerting

Two Ways to Improve Mobile Device Security Now

Ensure all employee devices, whether personal or corporate-owned, are secured by MobileIron and not just ActiveSync.

Configure ActiveSync traffic to flow only through MobileIron Sentry to ensure unsecured or infected mobile devices can't access corporate data.



Mobile Threat:	How MobileIron Mitigates It:
Stagefright: Targets Android devices through infected MMS downloads.	Secure company email, apps and data with separately encrypted Android container.
Keyraider: Steals confidential data from jailbroken devices.	Detects and denies corporate access to jailbroken devices.
YiSpecter: Can modify, install, and launch iOS apps without the user's permission.	Identifies and quarantines devices running versions of iOS older than 8.4.

MobileIron and ecosystem partners:

XcodeGhost: Targets iOS devices through infected App Store apps.	Together with ecosystem partners like FireEye and Lookout identifies infected apps and quarantines devices running them.

Contact MobileIron at globalsales@mobileiron.com to learn more about these threats and find out how MobileIron can secure and protect mobile devices in your enterprise.

MobileIron