ECO-0 · Mobile Threat Catalogue

Archived: 2026-04-05 23:41:01 UTC

Mobile Threat Catalogue

Exploitation of PC Backups

Contribute

Threat Category: Mobile OS & Vendor Infrastructure

ID: ECO-0

Threat Description: Mobile device backup data that is stored on a user's personal computer may be exploited through weak passwords or other access methods. Mobile device data may also be inadvertently stolen when the mobile device is plugged into a compromised personal computer.

Threat Origin

Not Applicable, See Exploit or CVE Examples

Exploit Examples

BackStab: Mobile Backup Data Under Attack from Malware [1]

iOS 10: Security Weakness Discovered, Backup Passwords Much Easier to Break [2]

CVE Examples

Not Applicable

Possible Countermeasures

Mobile Device User

As knowledge of the authentication credentials for any associated account (e.g., iTunes, Google) may facilitate an attacker's ability to initiate, access, or decrypt device backups, follow best practices for management of device account passwords.

To detect malware that may realize this threat against device backups to a trusted computer, ensure up-to-date anti-malware software is configured to regularly scan for malicious files and application behavior.

To prevent this threat for backups to a trusted computer, configure any device backup software (e.g., iTunes) to encrypt all device backups. Furthermore, securely erase any unencrypted backups that may already exist.

To prevent a device from being inadvertently backed up to an computer under an attacker's control, when charging the device, do not grant trust to an untrusted computer or charging station.

To prevent an attacker from directly initiating an unauthorized device backup to a controlled computer, ensure a device unlock code has been configured for the device and that the device is left in a locked state when being left unattended.

To further prevent an attacker from directly initiating an unauthorized device backup to a controlled computer, use strong physical security measures (e.g., lock the device into a secure container) when leaving a device directly unattended.

Enterprise

To detect malware that may realize this threat against device backups to a trusted computer, ensure up-to-date anti-malware software is configured to regularly scan for malicious files and application behavior.

To prevent this threat for all backups of managed devices, deploy EMM/MDM solutions in combination with devices that successfully enforce policies to either encrypt all device backups or to block device backups entirely, as appropriate.

To prevent this threat for enterprise data contained in backups of managed devices, deploy EMM/MDM/container solutions in combination with devices that successfully enforce policies to either encrypt all enterprise data, or block enterprise data from being included in device backups.

References

1. C. Xiao, "BackStab: Mobile Backup Data Under Attack from Malware", paloalto, 7 Dec. 2015; http://researchcenter.paloaltonetworks.com/2015/12/backstab-mobile-backup-data-under-attack-from-malware/ [accessed 8/29/2016] ↩

2. O. Afononin, *TouchLogger: Inferring Keystrokes on Touch Screen from Smartphone Motion*, Elcomsoft Blog, 23 Sept 2016; https://blog.elcomsoft.com/2016/09/ios-10-security-weakness-discovered-backup-passwords-much-easier-to-break/ [accessed 12/9/2016] ↩
