ระวังภัย พบโปรแกรม Xcode ปลอม แอบฝังโค้ดอันตรายลงในแอป iOS ผู้ใช้ WeChat ได้รับผลกระทบ

เรื่อง: ระวังภัย พบโปรแกรม Xcode ปลอม แอบฝังโค้ดอันตรายลงในแอป iOS ผู้ใช้ WeChat ได้รับผลกระทบ
ประเภทภัยคุกคาม: Malicious Code

เมื่อวันที่ 17 กันยายน 2558 นักวิจัยด้านความมั่นคงปลอดภัยจากบริษัท Palo Alto Networks สหรัฐอเมริกา ได้รายงานการค้นพบมัลแวร์ชื่อ XcodeGhost ซึ่งเป็นการนำโปรแกรม Xcode ของ Apple มาแก้ไขใหม่ โดยให้โปรแกรม Xcode แอบเพิ่มโค้ดอันตรายลงในแอปพลิเคชัน iOS ที่นักพัฒนาเผยแพร่ด้วย ซึ่งโค้ดอันตรายดังกล่าวมีทั้งแอบขโมยข้อมูลส่วนตัวหรือหลอกขโมยชื่อผู้ใช้/รหัสผ่าน [1]

Xcode เป็นโปรแกรมสำหรับใช้พัฒนาแอปพลิเคชันบนระบบปฏิบัติการณ์ iOS ซึ่งโปรแกรมนี้ต้องติดตั้งบนระบบปฏิบัติการ Mac OS X เนื่องจากไฟล์ติดตั้งโปรแกรม Xcode มีขนาดใหญ่ และนักพัฒนาต้องดาวน์โหลดโปรแกรมนี้มาจากเซิร์ฟเวอร์ของ Apple ซึ่งหลายๆ ภูมิภาคในประเทศจีนนั้นการเชื่อมต่ออินเทอร์เน็ตไปยังเซิร์ฟเวอร์ต่างประเทศเป็นไปได้ช้า ทำให้นักพัฒนาบางส่วนเลือกที่จะดาวน์โหลดซอฟต์แวร์จากแหล่งดาวน์โหลดภายในประเทศแทน

จากรายงานของบริษัท Palo Alto Networks ระบุว่ามีผู้อัปโหลดโปรแกรม Xcode เวอร์ชันดัดแปลงขึ้นไปไว้บนเซิร์ฟเวอร์ที่ให้บริการฝากไฟล์แห่งหนึ่งในประเทศจีน โดยโปรแกรม Xcode เวอร์ชันดัดแปลงนี้จะลักลอบเพิ่มโค้ดลงในแอปพลิเคชัน iOS ที่ผู้ใช้พัฒนาอยู่ เมื่อมีการคอมไพล์ซอร์สโค้ดโปรแกรม Xcode จะใส่โค้ดสำหรับขโมยข้อมูลส่วนตัวหรือหลอกขโมยชื่อผู้ใช้/รหัสผ่านลงในแอปพลิเคชันนั้นด้วย ซึ่งกรณีนี้นักพัฒนาจะไม่ทราบถึงความผิดปกติ และเมื่อมีการส่งแอปพลิเคชันขึ้นไปบน App Store ก็มีโอกาสที่จะผ่านกระบวนการตรวจสอบของ Apple และสามารถถูกดาวน์โหลดไปติดตั้งลงในเครื่องของผู้ใช้ได้โดยง่าย ซึ่งในกรณีนี้ ผู้ใช้งานอุปกรณ์ iOS ที่ไม่ได้ Jailbreak ก็สามารถติดมัลแวร์ได้

ทางบริษัท Palo Alto Networks ได้เปิดเผยรายชื่อแอปพลิเคชันที่ได้รับผลกระทบจากการที่นักพัฒนาใช้โปรแกรม Xcode เวอร์ชันดัดแปลง โดยหนึ่งในนั้นมีรายชื่อแอปพลิเคชัน WeChat ซึ่งเป็นแอปพลิเคชันสนทนาที่มีผู้ใช้งานในประเทศไทยพอสมควร

ผลกระทบ

ผู้ใช้งานอุปกรณ์ iOS ซึ่งทำการติดตั้งแอปพลิเคชันที่ถูกแอบฝังโค้ดอันตราย อาจถูกขโมยข้อมูลส่วนตัวหรือถูกหลอกขโมยชื่อผู้ใช้/รหัสผ่านได้ [2]

ระบบที่ได้รับผลกระทบ

ผู้ใช้งานอุปกรณ์ iOS ที่ติดตั้งแอปพลิเคชันที่ถูกแอบฝังโค้ดอันตราย โดยทาง Palo Alto Networks Fox-it แจ้งว่ามีประมาณมากกว่า 50 แอปพลิเคชัน [1] ตัวอย่างรายชื่อแอปพลิเคชันที่ได้รับผลกระทบ เช่น

- WeChat เวอร์ชัน 6.2.5 [3]
- WinZip
- CamScanner
- CamCard
- Oplayer
- PDFReader
- Perfect365

ข้อแนะนำในการป้องกันและแก้ไข

ปัจจุบันโปรแกรม Xcode เวอร์ชันดัดแปลงถูกลบออกจากเซิร์ฟเวอร์ที่ให้บริการฝากไฟล์ดังกล่าวแล้ว[1] รวมถึงแอปพลิเคชัน iOS ที่ติดมัลแวร์ก็ถูก Apple นำถอดออกจาก App Store เป็นการชั่วคราวแล้วเช่นกัน [4]

สำหรับนักพัฒนา ควรตรวจสอบว่าดาวน์โหลดโปรแกรม Xcode หรือโปรแกรมอื่นๆ ที่ใช้ในการพัฒนาแอปพลิเคชัน จากแหล่งที่มาที่น่าเชื่อถือ เช่น จากเว็บไซต์ของผู้พัฒนาโดยตรง [5] หากพบว่าโปรแกรมที่ติดตั้งอยู่มาจากแหล่งที่มาที่ไม่แน่ใจ ควรถอนการติดตั้งและดาวน์โหลดมาติดตั้งใหม่

สำหรับผู้ใช้งานอุปกรณ์ iOS ควรตรวจสอบรายชื่อแอปพลิเคชันที่ได้รับผลกระทบ หากยังไม่มีการเผยแพร่อัปเดต ควรลบแอปพลิเคชันดังกล่าวออกจากเครื่องก่อนเพื่อความปลอดภัย รวมถึงเปลี่ยนรหัสผ่าน Apple ID และบัญชีต่าง ๆ ที่มีการใช้งาน

หมายเหตุ: ปัจจุบันผู้พัฒนาแอปพลิเคชัน WeChat มีการประกาศอัปเดตเวอร์ชันที่มีการแก้ไขปัญหาแล้ว ผู้ใช้งานสามารถอัปเดตเป็นเวอร์ชัน 6.2.6 ได้ทันที ตามประกาศ[3]

อ้างอิง

1. http://researchcenter.paloaltonetworks.com/2015/09/malware-xcodeghost-infects-39-ios-apps-including-wechat-affecting-hundreds-of-millions-of-users/
2. http://researchcenter.paloaltonetworks.com/2015/09/update-xcodeghost-attacker-can-phish-passwords-and-open-urls-though-infected-apps/
3. http://blog.wechat.com/2015/09/19/fixed-security-flaw-in-wechat-v6-2-5-for-ios/
4. http://www.bbc.com/news/technology-34311203
5. https://developer.apple.com/xcode/download