แจ้งเตือน :
Malware บน Google Play Store

ผลกระทบทางธุรกิจ
- ☒ Financial damage
- ☒ Reputation damage
- ☐ Non-compliance
- ☐ Privacy violation

ผลกระทบต่อระบบ
- ☒ Loss of Confidentiality
- ☒ Loss of Integrity
- ☐ Loss of Availability

TLP Color : White
(Traffic Light Protocol)

ผู้รับสามารถเผยแพร่ข้อมูลสู่สาธารณะได้

ข่าวการแจ้งเตือน Malware บน Google Play Store ที่มีวัตถุประสงค์ขโมยข้อมูล

วันที่แจ้งเตือน 16 มิถุนายน 2565

ด้วยศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ศปช. สกมช.) ได้แจ้งข่าวนักวิจัยด้านความปลอดภัยทางไซเบอร์ในต่างประเทศ ค้นพบแอปพลิเคชันที่เป็น adware และ malware ที่มีวัตถุประสงค์ในการขโมยข้อมูลจากเครื่องผู้ใช้งาน อย่างน้อย 5 แอปพลิเคชัน ใน Google Play Store

ทั้งนี้ malware ดังกล่าวจะพยายามซ่อนตัว เพื่อขโมยข้อมูลของเหยื่อไม่เพียงแต่ login credentials sites ที่เหยื่อใช้งานบ่อย ๆ ซึ่งรวมถึง social media และบัญชีธุรกรรม online ต่าง ๆ หรือขโมยข้อมูลจากการแจ้งเตือน (notifications) ของแอปพลิเคชันอื่น ๆ เพื่อเอารหัสผ่าน 2FA แบบ One-Time-Passcode ได้อีกด้วย

รายชื่อ 5 แอปพลิเคชันดังกล่าวยังคงสามารถดาวน์โหลดได้จาก Google Play Store มีดังนี้

- **PIP Pic Camera Photo Editor** – 1 million downloads, malware masquerading as image-editing software, but which steals the Facebook account credentials of its users.
- **Wild & Exotic Animal Wallpaper** – 500,000 downloads, an adware trojan that replaces its icon and name to 'SIM Tool Kit' and adds itself to the battery-saving exceptions list.
- **ZodiHoroscope** – Fortune Finder – 500,000 downloads, malware that steal Facebook account credentials by tricking users into entering them, supposedly to disable in-app ads.
- **PIP Camera 2022** – 50,000 downloads, camera effects app that is also a Facebook account hijacker.
- **Magnifier Flashlight** – 10,000 downloads, adware app that serves videos and static banner ads.

ผู้ดูแลระบบควรเฝ้าระวัง หรือสื่อสารกับพนักงานและผู้ใช้บริการ (หากจำเป็น) เพื่อหลีกเลี่ยงและป้องกันความเสี่ยงและภัยคุกคามที่อาจจะเกิดขึ้น จากการที่พนักงานหรือผู้ใช้บริการที่ทำธุรกรรมผ่าน mobile device อาจจะไม่ทราบและไม่ตระหนักถึงความเสี่ยงจากดาวน์โหลดแอปพลิเคชันดังกล่าว

ข้อมูลอ้างอิง :

(1) https://www.bleepingcomputer.com/news/security/android-malware-on-the-google-play-store-gets-2-million-downloads/

(2) ข้อมูลจากศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ศปช. สกมช.) วันที่ 16 มิ.ย. 65

ประจำวันพฤหัสบดีที่ 16 มิถุนายน 2565

มัลแวร์ Android บน Google Play Store มียอดดาวน์โหลดมากถึง 2 ล้านครั้ง

นักวิจัยด้านความปลอดภัยทางไซเบอร์ได้ค้นพบแอปพลิเคชันที่เป็นแอดแวร์และมัลแวร์ที่ขโมยข้อมูล บน Google Play Store เมื่อเดือนที่แล้ว โดยมีอย่างน้อย 5 แอป โดยยังคงมีให้ใช้งานได้ และมียอดดาวน์โหลดมากกว่า 2 ล้านครั้ง โดยจะทำให้แบตเตอรีหมดไว สร้างความร้อน และแม้กระทั่งทำให้เกิดค่าใช้จ่ายโดยที่ผู้ใช้งานไม่ได้รับอนุญาต ตัวซอฟต์แวร์นี้มักจะพยายามซ่อนโดยปลอมแปลงเป็นอย่างอื่นบนอุปกรณ์ และสร้างรายได้ให้กับผู้ให้บริการระยะไกลโดยบังคับให้เหยื่อทำการดูหรือคลิกโฆษณาในเครือ อย่างไรก็ตาม โทรจันที่ขโมยข้อมูลนั้นจะเลวร้ายกว่ามาก โดยเป็นการขโมยข้อมูลรับรองการเข้าสู่ระบบสำหรับเว็บไซต์อื่นๆ ที่คุณเข้าไปใช้งานบ่อย รวมถึงการเข้าสู่บัญชีโซเชียลมีเดีย และบัญชีธนาคารออนไลน์ของคุณอีกด้วย

นักวิจัยรายงานว่าแอปพลิเคชันแอดแวร์และโทรจันที่ขโมยข้อมูลเป็นหนึ่งในภัยคุกคาม Android ที่โดดเด่นที่สุดในเดือนพฤษภาคม 2565 ในบรรดาภัยคุกคามมากมายที่สามารถแทรกซึมเข้าไปใน Google Play Store ยังคงมีอยู่ 5 รายการ ต่อไปนี้ :

1. PIP Pic Camera Photo Editor – จำนวนดาวน์โหลด 1 ล้านครั้ง มัลแวร์ปลอมแปลงเป็นซอฟต์แวร์แก้ไขรูปภาพ แต่ขโมยข้อมูลประจำตัวของบัญชี Facebook ของผู้ใช้
2. Wild & Exotic Animal Wallpaper – จำนวนดาวน์โหลด 500,000 ครั้ง ซึ่งเป็นแอดแวร์โทรจันที่แทนที่ไอคอนและชื่อเป็น 'SIM Tool Kit' และเพิ่มตัวเองลงในรายการข้อยกเว้นการประหยัดแบตเตอรี่
3. ZodiHoroscope – Fortune Finder – จำนวนดาวน์โหลด 500,000 ครั้ง มัลแวร์ที่ขโมยข้อมูลประจำตัวของบัญชี Facebook โดยหลอกให้ผู้ใช้ป้อนข้อมูลเหล่านี้ ซึ่งคาดว่าจะปิดการใช้งานโฆษณาในแอป
4. PIP Camera 2022 – จำนวนดาวน์โหลด 50,000 ครั้ง แอปพลิเคชันเอฟเฟกต์กล้องที่จะขโมยข้อมูลบัญชี Facebook
5. Magnifier Flashlight – จำนวนดาวน์โหลด 10,000 ครั้ง แอปแอดแวร์ที่ให้บริการวิดีโอและโฆษณาแบนเนอร์

ที่มาของข่าว : https://www.bleepingcomputer.com/news/security/android-malware-on-the-google-play-store-gets-2-million-downloads/