แจ้งเตือน : Malware

HIGH

ผลกระทบทางธุรกิจ

- [x] Financial Damage
- [x] Reputation Damage
- [ ] Non-compliance
- [x] Privacy Violation

ผลกระทบต่อระบบ

- [x] Loss of Confidentiality
- [x] Loss of Integrity
- [x] Loss of Availability

TLP Color : White

ผู้รับสามารถเผยแพร่ข้อมูลสู่สาธารณะได้

แจ้งเตือน Malware Campaign ปลอมแปลง Android Application ให้ดูเหมือน Application จากหน่วยงานภาครัฐ

วันที่แจ้งเตือน 22 กันยายน 2565

เมื่อ วันที่ 12 กันยายน 2565 ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT) รายงานพบตัวอย่างโปรแกรมไม่หวังดีบนระบบแอนดรอยด์ (Android Remote Access Trojan (RAT)) ซึ่งมีเป้าหมายโจมตีผู้ใช้โทรศัพท์ระบบปฏิบัติการแอนดรอยด์ (Android OS) โดยการปลอมแปลงแอปพลิเคชันให้ดูเหมือนเป็นแอปพลิเคชันที่สร้างโดยหน่วยงานภาครัฐ (เช่น กรมสรรพากร กรมสอบสวนคดีพิเศษ) เพื่อหลอกให้ดาวน์โหลดและติดตั้งแอปพลิเคชันลงบนโทรศัพท์ และ ขโมยข้อมูลที่มีความอ่อนไหว (sensitive information) เช่น ชื่อ-นามสกุล หมายเลขโทรศัพท์ ข้อมูลบัญชีผู้ใช้งานและรหัสผ่านแอปพลิเคชันของธนาคาร และข้อมูลการเปลี่ยนแปลงของแอปพลิเคชันต่าง ๆ บนอุปกรณ์ของเหยื่อ

เพื่อหลีกเลี่ยงและป้องกันความเสี่ยงที่อาจเกิดขึ้น บริษัทควรแนะนำให้บุคลากรภายในองค์กรดำเนินการดังนี้

<u>คำแนะนำ</u>

- อัปเดตซอฟต์แวร์ป้องกันไวรัส (antivirus software) อยู่เสมอเพื่อตรวจจับและป้องกันการติดมัลแวร์
- อัปเดตระบบปฏิบัติการ (operating system) และแอปพลิเคชันในโทรศัพท์อย่างสม่ำเสมอ
- ใช้รหัสผ่านที่มีความซับซ้อน รัดกุม ยากต่อการคาดเดา และเปิดใช้งานการตรวจสอบสิทธิแบบสองปัจจัย (two-factor authentication) กับทุกระบบที่รองรับ
- ตรวจสอบ privileges และ permissions ที่แอปพลิเคชันร้องขอก่อนให้สิทธิเข้าถึงโทรศัพท์
- ดาวน์โหลดและติดตั้งซอฟต์แวร์จากแหล่งที่เชื่อถือได้และเป็น official เท่านั้น เช่น Google Play Store
- เปิดใช้งาน biometric security features เช่น ลายนิ้วมือ (fingerprint) หรือรหัสผ่านเพื่อปลดล็อกโทรศัพท์หากทำได้
- ระมัดระวังการเปิดลิงก์ใน SMS หรืออีเมลที่ส่งไปยังโทรศัพท์
- ตรวจสอบเพื่อให้แน่ใจว่าได้เปิดใช้งาน Google Play Protect บนโทรศัพท์ที่ใช้ Android OS แล้ว
- กรณีตรวจพบการทำธุรกรรมที่ผิดปกติของบัญชีธนาคาร ให้รีบแจ้งธนาคารเจ้าของบัญชีโดยเร็วที่สุด
- บริษัทควรให้ความรู้แก่ลูกค้า และ บุคลากรภายในองค์กรเกี่ยวกับการป้องกันตนเองจากการโจมตีจากมัลแวร์ผ่านอุปกรณ์โทรศัพท์เคลื่อนที่ SMS อีเมล หรือ voice phishing

แจ้งเตือน : Malware

HIGH

ผลกระทบทางธุรกิจ

- [x] Financial Damage
- [x] Reputation Damage
- [ ] Non-compliance
- [x] Privacy Violation

ผลกระทบต่อระบบ

- [x] Loss of Confidentiality
- [x] Loss of Integrity
- [x] Loss of Availability

TLP Color : White

ผู้รับสามารถเผยแพร่ข้อมูลสู่สาธารณะได้

แจ้งเตือน Malware Campaign ปลอมแปลง Android Application ให้ดูเหมือน Application จากหน่วยงานภาครัฐ (ต่อ)

วิธีตรวจสอบว่าโทรศัพท์ถูกโจมตีหรือไม่

- ตรวจสอบปริมาณการใช้ข้อมูลการเข้าถึงอินเทอร์เน็ตของ Cellula (3G/4G/5G) หรือ Wi-Fi ของแอปพลิเคชันที่ติดตั้งในโทรศัพท์เป็นประจำ
- ตรวจสอบการแจ้งเตือนจากซอฟต์แวร์ป้องกันไวรัส (antivirus software) หรือ การแจ้งเตือนจาก Android OS และดำเนินการต่าง ๆ ที่จำเป็นเพื่อแก้ไขปัญหาจากการแจ้งเตือน

หากตรวจสอบแล้วพบว่าถูกโจมตีจาก Android Remote Access Trojan (RAT) ควรดำเนินการดังนี้

- ปิดการใช้งาน (disable) Cellula (3G/4G/5G) หรือ Wi-Fi และนำซิมการ์ดออก เนื่องจากในบางกรณี Android Remote Access Trojan (RAT) อาจสามารถแอบเปิดใช้งานการเข้าถึงอินเทอร์เน็ตได้อีกครั้ง
- สำรองข้อมูล (backup) และรีเซ็ตโทรศัพท์ให้เป็นค่าจากโรงงาน (factory reset)
- ถอนการติดตั้งแอปพลิเคชันออก (uninstall) ในกรณีที่ไม่สามารถรีเซ็ตให้เป็นค่าจากโรงงานได้

ข้อมูลอ้างอิง

รายงานการแจ้งเตือนของศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT) วันที่ 12 กันยายน 2565 (https://drive.google.com/file/d/1hDlBQu-saeqlALq5H0FHHJu_EnC-0Dr2/view)