แจ้งเตือน

Alert

ผลกระทบทางธุรกิจ

- ☒ Financial Damage
- ☒ Reputation Damage
- ☒ Non-compliance
- ☒ Privacy Violation

ผลกระทบต่อระบบ

- ☒ Loss of Confidentiality
- ☒ Loss of Integrity
- ☒ Loss of Availability

TLP Color : CLEAR

ผู้รับสามารถเผยแพร่ข้อมูลสู่สาธารณะได้

แจ้งเตือนเพื่อเฝ้าระวังภัยคุกคามจาก Bluekit แพลตฟอร์มอาชญากรรมไซเบอร์ Phishing-as-a-Service (PHaaS)

วันที่แจ้งเตือน 1 กรกฎาคม 2569

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) ได้เผยแพร่รายงานเกี่ยวกับภัยคุกคามทางไซเบอร์ กรณี BlueKit ซึ่งเป็นแพลตฟอร์มอาชญากรรมทางไซเบอร์ในรูปแบบการให้บริการสำเร็จรูป Phishing-as-a-Service (PHaaS) โดยมีรายละเอียดดังนี้

การโจมตี	รายละเอียด
• Bluekit แพลตฟอร์ม Phishing-as-a-Service (PHaaS) เป็นชุดเครื่องมือที่ถูกพัฒนาขึ้นเพื่อช่วยให้อาชญากรไซเบอร์สามารถโจมตีและขโมยบัญชีผู้ใช้งาน • โดยใช้เทคนิค Browser-in-the-Middle (BitM) ที่สามารถหลีกเลี่ยงกลไกตรวจจับของระบบรักษาความมั่นคงปลอดภัย โดยสามารถข้ามผ่านกระบวนการยืนยันตัวตนแบบหลายปัจจัย (Multi-Factor Authentication: MFA) • ส่งผลให้หน่วยงานภาครัฐ เอกชน และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII) ที่ใช้งานบริการคลาวด์ มีความเสี่ยงระดับสูงที่จะถูกดักรับข้อมูลประจำตัวและถูกโจรกรรมสิทธิ์ในการเข้าถึงบัญชี โดยเฉพาะกลุ่มบัญชีที่ยังใช้ระบบ MFA รูปแบบเดิม เช่น การรับรหัสผ่านครั้งเดียวผ่าน SMS หรือแอปพลิเคชันบนโทรศัพท์เคลื่อนที่ เป็นต้น	• การแสดงหน้า login เข้าสู่ระบบยังเป็นเว็บไซต์จริงและสามารถใช้งานได้ตามปกติทำให้ผู้ใช้งานสังเกตความผิดปกติได้ยาก • การดักรับข้อมูลประจำตัวและรหัสผ่านเมื่อผู้ใช้งานทำการกรอกรหัสผ่านและรหัสยืนยันตัวตน เช่น OTP จาก SMS หรือ Authenticator เป็นต้น ทำให้ MFA รูปแบบเดิมไม่สามารถสกัดกั้นการโจมตีได้ • การขโมย Session เพื่อสวมรอย (Session Hijacking) หลังจากยืนยันตัวตนสำเร็จ Bluekit จะทำการคัดลอกคุกกี้ (Session Cookies) และส่งไปให้ผู้โจมตี ทำให้ผู้โจมตีสามารถสวมรอยเข้าสู่ระบบจากอุปกรณ์อื่นได้โดยไม่ต้องผ่านการพิสูจน์ตัวตน • มีการนำ AI มาใช้บริหารจัดการแคมเปญ เช่น การหลบเลี่ยงระบบตรวจสอบสิทธิ (CAPTCHA) การบิดเบือนโค้ดเพื่อหลบเลี่ยงการตรวจจับของระบบแอนตี้ไวรัส รวมถึงในบางกรณีพบการใช้เทคโนโลยีปลอมแปลงเสียง (Voice Cloning) เพื่อล่อลวงผู้เสียหาย

แนวทางการป้องกัน:

1. พิจารณาใช้งานระบบยืนยันตัวตน (Phishing-Resistant MFA): เพื่อป้องกันฟิชชิง เช่น การใช้อุปกรณ์ฮาร์ดแวร์ (Security Key ตามมาตรฐาน FIDO2 / WebAuthn) หรือระบบ Passkeys เป็นต้น เนื่องจากระบบดังกล่าวจะทำการผูกสิทธิเข้ากับโดเมนเนมที่ถูกต้องเท่านั้น ผู้ไม่หวังดีไม่สามารถนำคุกกี้เซสชันไปใช้สวมรอยต่อได้
2. การจำกัดอายุของเซสชัน (Session Timeout) กำหนดค่าอายุการใช้งานของ Session Cookies เพื่อให้ผู้ใช้งานต้องทำการพิสูจน์ตัวตนตามรอบเวลาที่เหมาะสม ซึ่งจะช่วยลดโอกาสและระยะเวลาในการสวมรอยของผู้โจมตี
3. การประเมินและตรวจสอบความปลอดภัยระบบ: จัดให้มีการบริหารจัดการสิทธิการเข้าถึงข้อมูลภายในองค์กร และการทดสอบเจาะระบบ (Penetration Testing) อย่างสม่ำเสมอ
4. ตรวจสอบ URL ก่อนกรอกชื่อผู้ใช้และรหัสผ่าน และหลีกเลี่ยงการเข้าสู่ระบบผ่านลิงก์ที่ไม่น่าเชื่อถือ
5. การปฏิเสธการยืนยันตัวตนที่ไม่ได้ทำธุรกรรมด้วยตนเอง: หากปรากฏหน้าต่างหรือข้อความแจ้งเตือนให้ระบุรหัส OTP หรือ อนุมัติการเข้าสู่ระบบ (MFA Prompt) โดยที่ผู้ใช้งานไม่ได้เป็นผู้ดำเนินการในขณะนั้น ให้ปฏิเสธการกรอกข้อมูล และแจ้งผู้ดูแลระบบเพื่อตรวจสอบ

ข้อมูลอ้างอิง

1. รายงานการแจ้งเตือนของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ ประจำวันที่ 1 ก.ค. 2569
2. https://hackread.com/bluekit-phishing-uses-browser-in-the-middle-attacks/?