แจ้งเตือน : เฝ้าระวัง

Alert

ผลกระทบทางธุรกิจ

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

ผลกระทบต่อระบบ

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

TLP Color : CLEAR

ผู้รับสามารถเผยแพร่ข้อมูลสู่สาธารณะได้

เฝ้าระวังการนำ AI Agent มาใช้ในการโจมตีทางไซเบอร์

วันที่แจ้งเตือน 27 กรกฎาคม 2569

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

ThaiCERT สกมช. ได้เผยแพร่รายงานความเสี่ยงด้านภัยคุกคามไซเบอร์ กรณีการโจมตีทางไซเบอร์ที่ผู้ไม่หวังดีนำ Hermes Agent ซึ่งเป็น Autonomous AI Agent แบบ Open source มาใช้ร่วมกับมัลแวร์ Hades เพื่อสำรวจข้อมูลระบบและเครือข่าย ค้นหาช่องทางยกระดับสิทธิ รวบรวมข้อมูล เข้าถึงและคงอยู่ระบบเพื่อสื่อสารกับ Server ควบคุม (Command-and-Control: C2) โดยอัตโนมัติ ทำให้ผู้ไม่หวังดีสามารถทำการโจมตีได้อย่างรวดเร็ว ต่อเนื่องและลดขั้นตอนการสั่งการจากมนุษย์

AI Agent สามารถดำเนินการสำรวจระบบ ค้นหาบริการและไฟล์สำคัญ วิเคราะห์โครงสร้างเครือข่าย ตรวจสอบช่องทางยกระดับสิทธิ และใช้เครื่องมือหรือช่องโหว่ที่เตรียมไว้เพื่อขยายการโจมตีไปยังระบบอื่นภายในเครือข่าย ขณะที่มัลแวร์ Hades รองรับการควบคุมจากระยะไกล รับ-ส่งไฟล์ สร้างช่องทางการสื่อสารแบบเข้ารหัส และเข้าถึงและคงอยู่ระบบเพื่อระบบ ทำให้การตรวจสอบและตอบสนองต่อเหตุการณ์มีความซับซ้อนมากยิ่งขึ้น ซึ่งสะท้อนว่า AI Agent มีแนวโน้มถูกนำมาใช้เป็นเครื่องมือเพิ่มประสิทธิภาพในการโจมตีทางไซเบอร์เพิ่มมากขึ้น

ข้อแนะนำสำหรับองค์กร

มาตรการ	แนวทางปฏิบัติ
การควบคุมการเข้าถึง	เปิดใช้ Multi-Factor Authentication (MFA) โดยเฉพาะบัญชีผู้ดูแลระบบ จำกัดสิทธิตามหลัก Least Privilege และทบทวนบัญชีผู้ใช้งานสิทธิสูงอย่างสม่ำเสมอ
การบริหารจัดการช่องโหว่	อัปเดตแพตช์และแก้ไขช่องโหว่ของระบบที่เปิดให้บริการจากอินเทอร์เน็ต รวมถึงระบบบริหารจัดการและซอฟต์แวร์สำคัญโดยเร็ว
การเฝ้าระวังและการตรวจจับ	ติดตามพฤติกรรมผิดปกติของระบบ บัญชีผู้ใช้ และการเชื่อมต่อขาออก (Outbound Traffic) พร้อมใช้ EDR, XDR, NDR และ SIEM เพื่อช่วยตรวจจับการโจมตี
การลดพื้นที่การโจมตี	แบ่งแยกเครือข่าย (Network Segmentation) จำกัดการเข้าถึงระบบพัฒนา (Test Environment) และระบบสำคัญ (Critical System) ตรวจสอบ Web Shell เครื่องมือควบคุมระยะไกล และไฟล์ที่ไม่ทราบแหล่งที่มา
การกำกับดูแล AI	หากมีการใช้งาน AI Agent ภายในองค์กร ควรกำหนดขอบเขตและสิทธิ์การทำงานอย่างชัดเจน จัดเก็บ Audit Log และกำหนด Human Approval สำหรับการดำเนินการที่มีความเสี่ยงสูง
การตอบสนองและการกู้คืน	ทบทวนและซักซ้อมแผน Incident Response พร้อมสำรองข้อมูลตามหลัก 3-2-1-1-0 โดยแยกบัญชีและระบบสำรองออกจากระบบหลัก (3 สำเนา 2 สื่อ และเก็บ Off-site) รวมทั้งเพิ่มการจัดเก็บสำเนาแบบ Offline หรือ Immutable และทดสอบการกู้คืนข้อมูลอย่างสม่ำเสมอ

ข้อมูลอ้างอิง

1. รายงานการแจ้งเตือนของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ ประจำวันที่ 26 กรกฎาคม 2569