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

แจ้งเตือน คำแนะนำด้านความปลอดภัย กรณี Threat Actor กลุ่ม APT40 และ กลุ่ม APT41

วันที่แจ้งเตือน 13 สิงหาคม 2567

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศ ของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) สำนักงาคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ได้เผยแพร่แจ้งเตือนและให้คำแนะนำด้านความปลอดภัยทางไซเบอร์กรณีกลุ่ม Threat Actor APT40 และ APT41 ซึ่งมีเป้าหมายการโจมตีองค์กรในหลายอุตสาหกรรมหลายประเทศ โดย

● กลุ่ม APT40 มุ่งโจมตีโดยใช้ประโยชน์จากช่องโหว่ใหม่ ๆ เป็นช่องทางโจมตีได้อย่างรวดเร็ว ทันทีที่ช่องโหว่นั้น มีการเผยแพร่เป็น CVE เช่น Log4J, Atlassian Confluence และ Microsoft Exchange อีกทั้งกลุ่ม APT40 จะเก็บข้อมูลระบบของเครือข่ายที่สำคัญ เพื่อหาช่องทางในการเข้าถึงระบบ และหาช่องโหว่ของอุปกรณ์ซอฟท์แวร์ที่หมดอายุ หรือระบบที่ไม่มีการดูแลรักษา โดยจะทำการโจมตีอุปกรณ์นั้นทันที เช่น อุปกรณ์ IoT และ SOHO (Small Office/Home Office) ที่อยู่ในช่วง End of Life : EOL (สามารถดูข้อมูล IoC ได้จากข้อมูลอ้างอิง 2)

● กลุ่ม APT41 มุ่งเป้าโจมตีไปที่หน่วยงานด้านการขนส่งและโลจิสติกส์ สื่อและบันเทิง เทคโนโลยี และยานยนต์ โดยใช้ ANTSWORD ร่วมกับ BLUEBEAM Web Shell เพื่อเจาะระบบและขโมยข้อมูล (สามารถดูข้อมูล IoC ได้จากข้อมูลอ้างอิง 3)

ขอแนะนำให้หน่วยงาน ป้องกันการถูกโจมตี ดังนี้

1. เฝ้าระวังและตรวจสอบเหตุการณ์ด้านความปลอดภัยที่อาจเป็นอันตรายต่อระบบสารสนเทศ และอุปกรณ์ที่อยู่ในช่วง EOL
2. ป้องกันการถูกโจมตีและตรวจสอบการเข้าถึงระบบโดยไม่ได้รับอนุญาต
3. ตรวจสอบและปิดช่องโหว่ในระบบอย่างสม่ำเสมอ โดยเฉพาะช่องโหว่ที่เพิ่งมีการเปิดเผย
4. อัปเดตระบบปฏิบัติการ และโปรแกรมป้องกันมัลแวร์อย่างสม่ำเสมอให้เป็นเวอร์ชันล่าสุด
5. สำรองข้อมูลสำคัญและเก็บแยกจากระบบหลัก

สำนักงาน ก.ล.ต. เล็งเห็นถึงความเสี่ยงและภัยคุกคามที่อาจเกิดต่อผู้ประกอบธุรกิจในตลาดทุน จึงขอแจ้งข้อมูลดังกล่าวให้ผู้ประกอบธุรกิจทราบและพิจารณาดำเนินการตามความเหมาะสม เพื่อลดความเสี่ยงและผลกระทบที่อาจจะเกิดขึ้นกับการปฏิบัติงานของบริษัท

ข้อมูลอ้างอิง

1) รายงานการแจ้งเตือนของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ ประจำวันที่ 9 ส.ค. 2567
2) https://cloud.google.com/blog/topics/threat-intelligence/apt41-arisen-from-dust
3) https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-190a