แจ้งเตือน : เฝ้าระวัง

Alert

ผลกระทบทางธุรกิจ

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

ผลกระทบต่อระบบ

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

TLP Color : CLEAR



ผู้รับสามารถเผยแพร่ข้อมูลสู่สาธารณะได้

การเฝ้าระวังการโจมตีโดยใช้ AI Agent เพื่อขโมยข้อมูล AWS Credential

วันที่แจ้งเตือน 13 พฤศจิกายน 2569

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (สำนักงาน ก.ล.ต.) และศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ภาคตลาดทุน (TCM-CERT) ได้ติดตามข่าวสารและพบกรณีนักวิจัยด้านความปลอดภัยไซเบอร์ได้รายงานข้อมูลที่พบว่ามีการนำ AntiFox ซึ่งเป็นแพลตฟอร์ม Agentic AI สำหรับการทดสอบเจาะระบบ (Penetration Testing) ที่พุ่งเป้าโจมตี Web Service และระบบ Cloud ของ Amazon Web Services (AWS) โดยพบโครงสร้างพื้นฐานที่เกี่ยวข้องกับการโจมตีถูกติดตั้งบน Alibaba Cloud และถูกใช้ค้นหาช่องโหว่ สำรวจข้อมูลการตั้งค่าระบบ ติดตั้ง Web Shell และค้นหา Credential เพื่อการเข้าถึง AWS

จากการตรวจพบเหตุการณ์โจมตีพบว่า ผู้ไม่หวังดีจะติดตั้ง ASPX Web Shell บน Microsoft Internet Information Services (IIS) ที่เปิดให้เข้าถึงจากอินเทอร์เน็ต และค้นหาไฟล์การตั้งค่าของแอปพลิเคชัน ข้อมูล Database Connection String ตลอดจนข้อมูลและไฟล์บันทึกเหตุการณ์ที่อาจมีข้อมูลสำคัญก่อนนำข้อมูลดังกล่าวไปใช้เพื่อขยายผลการโจมตีไปยังระบบอื่น

นอกจากนี้ พบว่ามีการนำ AWS Credentials ที่สามารถใช้งานได้จริง รวมถึงได้นำ IAM User และ EC2 Role ไปใช้เรียก AWS API จำนวนมาก โดยมีการสลับใช้งานหลาย Identity และส่งคำขอ API หลายร้อยรายการภายในเวลาประมาณ 30 นาที แม้คำขอส่วนใหญ่จะถูกปฏิเสธ แต่ผู้โจมตียังสามารถเข้าถึงข้อมูลระบบ Production ได้สำเร็จ รวมทั้งพบการใช้ AWS Identity ที่ถูกต้องเพื่อ อ่าน คัดลอก และลบข้อมูลใน Amazon S3

ทั้งนี้ AWS ชี้แจงว่า เหตุการณ์ดังกล่าว ไม่ได้เกิดจากการที่บริการ AWS ถูกเจาะระบบโดยตรง แต่เป็นกรณีที่ผู้ไม่หวังดีนำ Credentials ที่ได้จากแอปพลิเคชันของลูกค้าที่ถูกโจมตีไปใช้เข้าถึง AWS Account ที่เกี่ยวข้อง

ข้อมูลอ้างอิง

1. https://github.com/AntiFox-AI/antifox/blob/main/README.en.md
2. https://www.bleepingcomputer.com/news/security/hackers-use-antifox-ai-agents-in-aws-credential-theft-attacks/

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

การเฝ้าระวังการโจมตีโดยใช้ AI Agent เพื่อขโมยข้อมูล AWS Credential

วันที่แจ้งเตือน 13 พฤศจิกายน 2569

ผู้ประกอบธุรกิจที่ใช้งาน AWS หรือมีระบบ Web Application ที่เชื่อมต่อกับ Cloud ควรพิจารณาดำเนินการ ดังนี้

แนวทางป้องกันและลดความเสี่ยง

1. ตรวจสอบระบบที่เปิดให้เข้าถึงจากอินเทอร์เน็ต โดยเฉพาะ Web Server และ Microsoft IIS เพื่อค้นหาร่องรอยการถูกโจมตี การติดตั้ง Web Shell หรือการดำเนินคำสั่งที่ผิดปกติ รวมถึงพิจารณาความสัมพันธ์ระหว่างเหตุการณ์บน Web Server กับกิจกรรมการเข้าถึง AWS ที่ผิดปกติ
2. ตรวจสอบ AWS API Activity และ Identity โดยเฉพาะกรณีที่พบ API Request จำนวนมากในช่วงเวลาสั้น ๆ การสลับใช้งานหลาย IAM Identity หรือพบคำขอที่ถูกปฏิเสธจำนวนมากสลับกับคำขอที่สำเร็จ ซึ่งอาจเป็นสัญญาณของการทดสอบสิทธิ์หรือค้นหาทรัพยากรภายใน Cloud
3. หลีกเลี่ยงการจัดเก็บ Long-term Access Key หรือข้อมูลลับไว้ใน Application Configuration และตรวจสอบไฟล์ Configuration, Backup, Log และ Source Code ว่าไม่มี AWS Access Key, Secret Access Key, Database Credential หรือ Secret อื่นที่อาจถูกนำไปใช้ขยายผลการโจมตี AWS แนะนำให้ ไม่นำ Long-term Access Key ไปไว้ใน Application Configuration
4. จำกัดสิทธิของ IAM ตามหลัก Least Privilege เพื่อให้แต่ละ User, Role และ Workload สามารถเข้าถึงเฉพาะทรัพยากรและดำเนินการเฉพาะที่จำเป็น ซึ่งจะช่วยลดผลกระทบกรณี Credential ถูกขโมย โดย AWS ระบุ Least Privilege เป็นหนึ่งในมาตรการสำคัญสำหรับการรับมือความเสี่ยงดังกล่าว
5. ใช้งาน Instance Metadata Service Version 2 (IMDSv2) เพื่อลดความเสี่ยงจากการเข้าถึง Instance Metadata และข้อมูล Credential ที่เชื่อมโยงกับ EC2 Role โดยไม่ได้รับอนุญาต
6. หากตรวจพบหรือสงสัยว่า Credential ถูกเปิดเผย ให้ยกเลิก Session และ Key ที่ได้รับผลกระทบ พร้อมเปลี่ยน Credentials และ Secrets Access Key ที่เกี่ยวข้องโดยเร็ว โดยเฉพาะข้อมูลที่เคยจัดเก็บหรือปรากฏอยู่ใน Application Configuration

สำนักงาน ก.ล.ต. และ TCM-CERT ตระหนักถึงความเสี่ยงจากภัยคุกคามทางไซเบอร์ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศและความต่อเนื่องในการดำเนินธุรกิจของหน่วยงานในภาคตลาดทุน จึงขอแจ้งข้อมูลดังกล่าวเพื่อให้หน่วยงานท่านพิจารณาดำเนินการเฝ้าระวังและเตรียมความพร้อมรับมือ เพื่อป้องกันหรือลดผลกระทบที่อาจเกิดขึ้นต่อการดำเนินธุรกิจ รวมทั้งการประสานงานกับหน่วยงานที่เกี่ยวข้อง ได้แก่ สำนักงาน ก.ล.ต. หรือหน่วยงานควบคุมหรือกำกับดูแลอื่น ๆ เพื่อให้หน่วยงานท่านสามารถตอบสนองได้อย่างทันท่วงที

ข้อมูลอ้างอิง

3. https://aviatrix.ai/threat-research-center/antifox-ai-pentesting-platform-aws-cloud-credential-theft-2026/
4. https://github.com/rtkwlf/wolf-tools/tree/main/pack_alerts/202611-antifox-alibaba-hosted-platforms-facilitate-web-cloud-intrusions