แจ้งเตือน :
ความเสี่ยงการโจมตีทางไซเบอร์จากกรณีความขัดแย้งระหว่างประเทศ

ผลกระทบทางธุรกิจ
- ☐ Financial damage
- ☒ Reputation damage
- ☐ Non-compliance
- ☐ Privacy violation

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

TLP Color : WHITE

ผู้รับสามารถเผยแพร่ข้อมูลสู่สาธารณะได้

แจ้งเตือนความเสี่ยงการโจมตีทางไซเบอร์จากกลุ่มที่ได้รับการสนับสนุนจากรัฐในกรณีความขัดแย้งระหว่างประเทศรัสเซียและยูเครน

วันที่แจ้งเตือน 17 มีนาคม 2565

ตามที่ได้แจ้งเตือนการโจมตีทางไซเบอร์จากกรณีความขัดแย้งระหว่างประเทศรัสเซียและยูเครน เมื่อวันที่ 3 และ 9 มีนาคม 2565 ที่ผ่านมานั้น ยังคงมีการรายงานการตรวจพบกิจกรรมของเครือข่ายผู้ไม่ประสงค์ดีเพิ่มขึ้นอย่างต่อเนื่องและขยายตัวไปยังประเทศหรือหน่วยงานที่ไม่ใช่คู่ขัดแย้ง และมีรายงานจากหน่วยงานความปลอดภัยไซเบอร์ระหว่างประเทศ (Cybersecurity and Infrastructure Security Agency : CISA) ตรวจพบการโจมตีจากกลุ่ม Hacker ที่ได้รับการสนับสนุนโดยรัฐ (State-Sponsored) โดยใช้การโจมตีประเภท Brute Force Attack ร่วมกับการ Bypass ขั้นตอนการยืนยันตัวตนแบบ MFA และดำเนินการยกระดับสิทธิจากการกำหนดค่าเริ่มต้นที่ไม่เหมาะสมร่วมกับช่องโหว่ PrintNightmare (CVE-2021-34527) เพื่อเข้าควบคุมเครื่องเป้าหมาย

<u>เพื่อหลีกเลี่ยงและป้องกันความเสี่ยงที่อาจเกิดขึ้น ผู้ดูแลระบบควรพิจารณาดำเนินการ ดังนี้</u>

1. ตรวจสอบการกำหนดค่าตั้งต้นของระบบยืนยันตัวตนแบบ MFA ให้มีการตรวจสอบยืนยันตัวตนอย่างเหมาะสมและปลอดภัยก่อนอนุญาตให้ผู้ใช้งานเพิ่มอุปกรณ์ใหม่ (Re-Enrollment) บนระบบ MFA ก่อนใช้งาน
2. กำหนดระยะเวลาและกำหนดจำนวนครั้งที่ต้องการให้ล็อกอิน และแก้ไขการรหัสผ่านให้ซับซ้อนคาดเดาได้ยาก
3. ตรวจสอบและยกเลิกบัญชีผู้ใช้งานในระบบที่ไม่ได้มีการใช้งาน (Dormant Account) บนระบบการยืนยันตัวตนแบบ MFA และบนเครื่อง Domain Controller
4. ตรวจสอบและอัปเดต Security Patch เพื่อแก้ไขช่องโหว่ของระบบปฏิบัติการและโปรแกรมที่ได้รับผลกระทบที่เกี่ยวข้อง
5. เฝ้าระวังและติดตามพฤติกรรมบัญชีผู้ใช้งานในการเข้าถึงระบบที่น่าสงสัยและเข้าระบบผิดพลาดหลายครั้ง และแจ้งเตือนผู้ที่เกี่ยวข้องได้ทันสถานการณ์
6. ตั้งค่าการตรวจจับและป้องกันการของการโจมตีในช่องทางต่าง ๆ ที่มีการรายงานในรายการ Indicator of Compromise (IOC) ได้แก่ IP Address ที่เกี่ยวข้อง เป็นต้น (จากข้อมูล Threat Intelligence ใน link ที่อ้างอิง)
7. ผู้ดูแลระบบควรประเมินความเสี่ยงจากการติดตั้ง Security Patch การตั้งค่าบนระบบการยืนยันตัวตนและเครื่อง Domain Controller และการป้องกันบนอุปกรณ์รักษาความปลอดภัยก่อนนำไปติดตั้งบนระบบที่ให้บริการจริง

แจ้งเตือน :
ความเสี่ยงการโจมตีทางไซเบอร์จากกรณีความขัดแย้งระหว่างประเทศ

ผลกระทบทางธุรกิจ
- ☒ Financial damage
- ☒ Reputation damage
- ☐ Non-compliance
- ☒ Privacy violation

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

TLP Color : WHITE

ผู้รับสามารถเผยแพร่ข้อมูลสู่สาธารณะได้

แจ้งเตือนความเสี่ยงการโจมตีทางไซเบอร์จากกลุ่มที่ได้รับการสนับสนุนจากรัฐในกรณีความขัดแย้งระหว่างประเทศรัสเซียและยูเครน

วันที่แจ้งเตือน 17 มีนาคม 2565

ข้อมูลอ้างอิง

1. https://www.cisa.gov/uscert/ncas/alerts/aa22-074a
2. https://www.cisa.gov/uscert/sites/default/files/publications/AA22-074A.stix.xml (IOC List)

External Link