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 เพื่อเฝ้าระวังการโจมตีโดยกลุ่ม Ransomware LOCKBIT โดยอาศัยช่องโหว่บน VMware ESXi (CVE-2021-21974) [เพิ่มเติมคำแนะนำ]

วันที่แจ้งเตือน 19 ธันวาคม 2566

ตามที่ ThaiCERT และ สำนักงานได้เผยแพร่รายงานเกี่ยวกับการแพร่ระบาดของ Ransomware LOCKBIT โดยอาศัยช่องโหว่บน VMware ESXi (CVE-2021-21974) ซึ่งผู้โจมตีสามารถเข้าถึงระบบได้โดยไม่ต้องผ่านการยืนยันตัวตน

ทั้งนี้ ThaiCERT ได้เผยแพร่ข้อมูล ยุทธวิธี เทคนิค และ ขั้นตอนการโจมตี (TTPs) รวมถึงข้อมูลบ่งชี้การถูกโจมตี (IoCs) ของกลุ่ม Ransomware LOCKBIT โดยสามารถ download เอกสารดังกล่าวได้ที่ https://www[.]cisa[.]gov/sites/default/files/2023-03/aa23-075a-stop-ransomware-lockbit.pdf รวมถึงคำแนะนำสำหรับการตรวจสอบเพื่อลดความเสี่ยงจากการถูกโจมตี คำแนะนำสำหรับการฝึกอบรมและสร้างความตระหนักของบุคลากรของหน่วยงาน และแนวทางปฏิบัติของบุคลากรของหน่วยงาน เพื่อลดความเสี่ยงจากการถูกโจมตี (เอกสารแนบท้าย) และเพื่อให้ผู้ประกอบธุรกิจได้นำข้อมูลดังกล่าวไปพิจารณาดำเนินการต่อไป

เพื่อลดโอกาสและความเสี่ยงที่อาจจะเกิดขึ้นกับองค์กรของท่าน สำนักงานจึงขอความร่วมมือผู้ประกอบธุรกิจภาคตลาดทุนทุกแห่ง เฝ้าระวัง และติดตาม ระบบงานสำคัญ รวมถึง สื่อสารความเสี่ยงดังกล่าวกับผู้ให้บริการภายนอกที่ให้บริการแก่องค์กรของท่าน โดยเฉพาะผู้ให้บริการภายนอกที่เข้าถึงหรือนำข้อมูลส่วนบุคคลขององค์กรท่านไปประมวลผลเพื่อป้องกันการถูกโจมตีจากกลุ่ม Ransomware ดังกล่าว

ข้อมูลอ้างอิง

1) รายงานการแจ้งเตือนของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ ประจำวันจันทร์ที่ 18 ธันวาคม 2566
2) รายงานการแจ้งเตือนของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ ประจำวันอาทิตย์ที่ 10 ธันวาคม 2566
3) [แจ้งเตือน] การโจมตีด้วย Ransomware แบบมุ่งเป้า VMware ESXi CVE-2021-21974 วันอังคารที่ 12 ธันวาคม 2566
4) [แจ้งเตือน] เพื่อเฝ้าระวังการโจมตีโดยกลุ่ม Ransomware LOCKBIT โดยอาศัยช่องโหว่บน VMware ESXi (CVE-2021-21974) วันพฤหัสบดีที่ 14 ธันวาคม 2566

คำแนะนำสำหรับการตรวจสอบเพื่อลดความเสี่ยงจากการถูกโจมตี

ลำดับ	คำแนะนำ	มี	ไม่มี
1	เก็บข้อมูลสำรองที่สำคัญอย่างสม่ำเสมอ โดยการแยกจากระบบเครือข่ายหลัก		
2	อัปเดตแพตช์และซอฟต์แวร์ รวมถึงระบบปฏิบัติการและโปรแกรมป้องกันไวรัส ตรวจสอบให้แน่ใจว่ามีการติดตั้งแพตช์ล่าสุดสำหรับ VMware ESXi และซอฟต์แวร์ที่เกี่ยวข้องทั้งหมด		
3	ติดตั้งโปรแกรมป้องกันไวรัส รวมถึงตรวจสอบการเข้าถึงของระบบเพื่อตรวจพบกิจกรรมที่ผิดปกติ และดำเนินการตอบสนอง		
4	ใช้ไฟวอลล์เพื่อกรองการส่งข้อมูลเข้าและออก แบ่งเครือข่ายเพื่อจำกัดการแพร่กระจายของมัลแวร์		
5	การเข้าสู่ระบบต้องมีการตรวจสอบหลายขั้นตอน (MFA) สำหรับการเข้าสู่ระบบเพื่อป้องกันการโจมตีด้วย Phishing สำหรับทุกการใช้งาน โดยเฉพาะเว็บเมล เครือข่าย และบัญชีการเข้าใช้งานที่สำคัญ		
6	ปิดการใช้งานสคริปต์มาโครจากไฟล์ทำงานที่ถูกส่งผ่านทางอีเมล		
7	ใช้ VPN สำหรับการเข้าถึงระบบทางไกลที่ปลอดภัย และตรวจสอบการกำหนดค่าโปรโตคอลเดสก์ท็อประยะไกล (RDP) อย่างสม่ำเสมอ		
8	ใช้เครื่องมือ EDR เพื่อตรวจหาและตอบสนองต่อความเสี่ยงอย่างสม่ำเสมอ		

คำแนะนำสำหรับการฝึกอบรมและตระหนักของบุคลากรของหน่วยงาน

ลำดับ	คำแนะนำ	มี	ไม่มี
1	จัดการฝึกอบรมเป็นประจำเกี่ยวกับการรับรู้ Phishing		
2	ให้ความรู้แก่พนักงานเกี่ยวกับการใช้งานเว็บไซต์อย่างปลอดภัย การใช้รหัสผ่านที่ปลอดภัย และความสำคัญของการไม่ดาวน์โหลดหรือติดตั้งซอฟต์แวร์ที่ไม่ได้รับอนุญาต		
3	ฝึกอบรมพนักงานให้รายงานกิจกรรมที่น่าสงสัยหรือการละเมิดที่อาจเกิดขึ้นทันที		

แนวทางปฏิบัติของบุคลากรของหน่วยงาน เพื่อลดความเสี่ยงจากการถูกโจมตี

ลำดับ	คำแนะนำ	มี	ไม่มี
1	พัฒนาและปรับปรุงแผนการตอบสนองต่อเหตุการณ์อย่างสม่ำเสมอ และดำเนินการฝึกซ้อมจำลองสถานการณ์เพื่อให้แน่ใจว่ามีความพร้อม		
2	ดำเนินการตรวจสอบความปลอดภัยเป็นระยะเพื่อระบุและลดความเสี่ยงจากช่องโหว่		
3	ตรวจสอบให้แน่ใจว่าผู้จำหน่ายปฏิบัติตามหลักปฏิบัติด้านความปลอดภัยทางไซเบอร์ที่เข้มงวด		
4	พิจารณาประกันภัยทางไซเบอร์เพื่อลดผลกระทบทางการเงินจากการโจมตีแรนซัมแวร์		
5	ปฏิบัติตามกฎระเบียบและมาตรฐานความปลอดภัยทางไซเบอร์ที่เกี่ยวข้อง		
6	ตรวจสอบเครือข่ายและระบบอย่างสม่ำเสมอเพื่อหากิจกรรมที่ผิดปกติ		

ลำดับ	คำแนะนำ	มี	ไม่มี
7	แบ่งปันข้อมูลด้านความปลอดภัยทางไซเบอร์ที่เกี่ยวข้องเพื่อรับข้อมูลภัยคุกคามล่าสุด		