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 การโจมตีด้วย DDoS Attack ของกลุ่ม Hacker จากประเทศกัมพูชา

วันที่แจ้งเตือน 11 กรกฎาคม 2566

เมื่อวันที่ 29 มิถุนายน – 3 กรกฎาคม 2566 ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ศปช.)[1] สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) และ ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT)[2] ได้เผยแพร่รายงานเกี่ยวกับประกาศปฏิบัติการ “OpThailand” ของกลุ่ม Hacker จากประเทศกัมพูชา ได้แก่ กลุ่ม Anonymous Cambodia กลุ่ม K0LzSec กลุ่ม Cyber Skeleton และกลุ่ม NDT SEC โดยใช้การโจมตีทางไซเบอร์แบบ Distributed Denial of Service (DDoS) Attack (วิธีการโจมตีระบบบนอินเตอร์เน็ต เพื่อทำให้ระบบปฏิเสธการทำงานหรือหยุดการทำงาน) โดยตั้งเป้าหมายไปยังหน่วยงานภาครัฐ และภาคเอกชนในประเทศไทย ผ่านข้อมูลจากระบบฐานข้อมูล หรือ IP Address ของหน่วยงานที่ตกเป็นเป้าหมาย ตามที่ปรากฏอยู่บนพื้นที่สาธารณะเพื่อใช้ในการโจมตี และมีการนำข้อมูลของหน่วยงานที่ถูกโจมตีไปเผยแพร่ต่อสาธารณะ ซึ่งเหตุการณ์ดังกล่าวอาจส่งผลให้เว็บไซต์บางส่วนของหน่วยงานไม่สามารถให้บริการได้ และก่อให้เกิดความเสียหายต่อหน่วยงานที่ถูกโจมตีในวงกว้าง

ศปช. แนะนำให้ผู้ดูแลระบบและผู้ใช้งานตรวจสอบความผิดปกติของระบบงานที่ให้บริการอยู่โดยทันที เพื่อหลีกเลี่ยงความเสี่ยงในการถูกโจมตีด้วย DDoS Attack [3]

TTC-CERT[4] แนะนำว่า ถึงแม้เว็บไซตของบางหน่วยงานจะมีการใช้บริการปองกันการโจมตีแบบ DDoS ของผู้ให้บริการภายนอกแล้วก็ตาม ไม่ควรประมาทและเตรียมการรับมือการโจมตีที่อาจเกิดขึ้นได้ในห่วงเวลานี้ โดย TTC-CERT มีคำแนะนำในการตรวจจับการโจมตีดังนี้

- การวิเคราะห์การเพิ่มขึ้นของ traffic
- การสร้างโปรไฟล traffic ขององคกรเบื้องตน (Baseline Traffic Profiling)
- การตรวจหาความผิดปกติที่เกิดจากอัตราการใชงาน (Rate-Based Anomalies)
- การตรวจหาความผิดปกติที่เกิดจากรูปแบบ (Pattern-Based Anomalies)
- การวิเคราะห์ทางภูมิศาสตร์ (Geographical Analysis)
- การแจงเตือนแบบเรียลไทม เป็นต้น

ข้อมูลอ้างอิง

1) รายงานการแจ้งเตือนของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ ประจำวันจันทร์ที่ 6 กรกฎาคม 2566
2) รายงานการแจ้งเตือนของศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT) ประจำวันที่ 3 กรกฎาคม 2566
3) https://nipa.cloud/th/blog/ddos-attack และ http://www2.crma.ac.th/itd/ThaiCERT/ThaiCERT23032017/index.asp
4) https://drive.google.com/file/d/1cbNArz5D-h1ckEAR-q20vu3Yl1CA5AFo/view