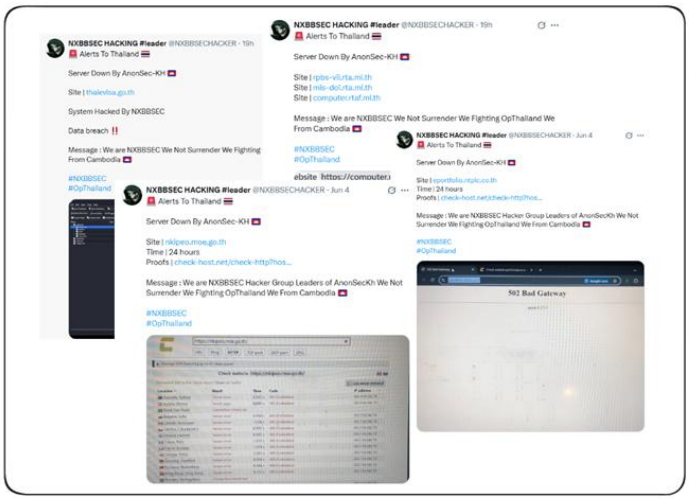
วันที่ 5 มิถุนายน 2568

กลุ่ม NXBBSEC จากกัมพูชา อ้างความรับผิดชอบต่อการโจมตีทางไซเบอร์ใส่เว็บไซต์ราชการไทยหลายแห่ง



Executive Summary

กลุ่ม Hacker ที่ใช้ชื่อว่า NXBBSEC HACKING อ้างตนว่าเป็นผู้นำของเครือข่าย AnonSec-KH จากประเทศกัมพูชา ได้ออกแถลงการณ์บนแพลตฟอร์ม X (Twitter) และ Telegram โดยประกาศอ้างความรับผิดชอบต่อการ โจมตีระบบเว็บไซต์ของหน่วยงานราชการไทยหลายแห่ง ภายใต้ปฏิบัติการที่เรียกว่า **#OpThailand** และได้มีข้อความจาก NXBBSEC ถึงประเทศไทยว่า "We are NXBBSEC Hacker Group Leaders of AnonSecKh We Not Surrender We Fighting OpThailand We From Cambodia" ซึ่งแปลได้ว่า พวกเราคือผู้นำกลุ่มแฮ็กเกอร์ NXBBSEC แห่ง AnonSecKH เราจะไม่ยอมแพ้ เราต่อสู้ในปฏิบัติการ OpThailand พวกเรามาจากกัมพูชา

เว็บไซต์ที่ถูกอ้างว่าโจมตีสำเร็จ ได้แก่

- http://nkipeo.moe[.]go[.]th – เว็บไซต์ของกระทรวงศึกษาธิการ
- http://thaievisa[.]go[.]th – ระบบลงทะเบียนขอวีซ่าออนไลน์ของไทย
- http://rpbs-vii.rta[.]mi[.]th – หน่วยงานในกองทัพบก
- http://mis-doi.rta[.]mi[.]th – หน่วยงานข้อมูลทหาร
- http://computer.rtaf[.]mi[.]th – ระบบสารสนเทศของกองทัพอากาศ
- https://eportfolio.ntplc[.]co[.]th – ระบบพอร์ตโฟลิโอบริษัทโทรคมนาคม

จากการตรวจสอบทางเทคนิคเบื้องต้น พบว่าในกรณีของเว็บไซต์ http://thaievisa[.]go[.]th มีหลักฐานการโจมตีที่สอดคล้องกับเครื่องมือสแกนช่องโหว่ที่ชื่อว่า "Wapiti" ที่ถูกใช้เพื่อสแกนหา ช่องโหว่ประเภท XSS, SQLi, และ LFI ซึ่งอาจนำไปสู่การเข้าควบคุมระบบหรือดึงข้อมูลสำคัญ และจากความเคลื่อนไหวล่าสุดพบว่า NXBBSEC เผยแพร่ลิงก์หลักฐานผ่านบริการ Check-host.net เพื่อแสดงผลว่าเว็บไซต์เป้าหมายไม่สามารถเข้าถึงได้ในช่วงเวลาที่อ้าง จากการตรวจสอบเพิ่มเติม พบว่าปัจจุบันเว็บส่วนใหญ่สามารถกลับเข้ามาใช้งานได้เป็นปกติ

คำแนะนำ (Recommendation)

- การเฝ้าระวังและติดตามกิจกรรมข่าวสารของกลุ่ม Hacker
- ดำเนินการตรวจสอบ Log server ย้อนหลังในช่วงเวลา 24–72 ชั่วโมง เพื่อตรวจสอบความผิดปกติ
- การอัปเดตแพตช์ระบบต่างๆ รวมถึงการตรวจสอบการจำกัดสิทธิ์การเข้าถึง

ข้อมูลอ้างอิง

- https://x.com/nxbbsechacker?lang=en