แจ้งเตือน : ความเสี่ยงการโจมตีทางไซเบอร์จากกรณีความขัดแย้งระหว่างประเทศ	ผลกระทบทางธุรกิจ	ผลกระทบต่อระบบ	TLP Color : WHITE
	☐ Financial damage ☒ Reputation damage ☐ Non-compliance ☐ Privacy violation	☒ Loss of Confidentiality ☒ Loss of Integrity ☒ Loss of Availability	 ผู้รับสามารถเผยแพร่ข้อมูลสู่สาธารณะได้

แจ้งเตือนความเสี่ยงการโจมตีทางไซเบอร์จากกรณีความขัดแย้งระหว่างประเทศรัสเซียและยูเครน

วันที่แจ้งเตือน 9 มีนาคม 2565

หลังจากการแจ้งเตือนการโจมตีทางไซเบอร์จากกรณีความขัดแย้งระหว่างประเทศรัสเซียและยูเครน และคำแนะนำในการป้องกันความเสี่ยงจากศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ศปช. สกมช.) เมื่อวันที่ 3 มีนาคม 2565 ยังมีรายงานการตรวจพบกิจกรรมฉวยโอกาสของเครือข่ายผู้ไม่หวังดีเพิ่มขึ้นอย่างต่อเนื่องและขยายไปยังประเทศหรือหน่วยงานที่ไม่ใช่คู่ขัดแย้ง เช่น การล่อลวงให้มีการดาวน์โหลด Malware ผ่าน e-Mail หลอกลวงโดยอ้างถึงสถานการณ์ดังกล่าว เป็นต้น

ก.ล.ต. ขอแจ้งข้อมูลและคำแนะนำที่เกี่ยวกับการโจมตีทางไซเบอร์ที่ได้รวบรวมจากแหล่งข้อมูลที่เป็นประโยชน์ เพื่อเฝ้าระวังการโจมตี ที่ฉวยโอกาสจากสถานการณ์โดยกลุ่มผู้ไม่หวังดีดังกล่าว ซึ่งมีรายละเอียดดังต่อไปนี้

1. ตั้งค่าการตรวจจับและป้องกันการของการโจมตีในช่องทางต่างๆที่มีการรายงานในรายการ Indicator of Compromise (IOC) ได้แก่ ค่า Hash ของเครื่องมือหรือไฟล์อันตราย URL และ IP Address ที่เกี่ยวข้อง เป็นต้น จากข้อมูล Threat Intelligence โดยสามารถศึกษารายละเอียดเพิ่มเติมได้จากแหล่งข้อมูลต่าง ๆ ดังนี้

1.1. https://www.trendmicro.com/en_us/research/22/c/cyberattacks-are-prominent-in-the-russia-ukraine-conflict.html

1.2. https://www.trendmicro.com/content/dam/trendmicro/global/en/research/22/c/cyberattacks-are-prominent-in-the-russia-ukraine-conflict/IOC%20Resource%20for%20Russia-Ukraine%20Conflict-Related%20Cyberattacks-03082022.pdf *External Link*

2. ผู้ดูแลระบบควรประเมินความเสี่ยงจากการตั้งค่าการป้องกันบนอุปกรณ์รักษาความปลอดภัยก่อนนำไปติดตั้งบนระบบที่ให้บริการจริง